

TITLE OF POLICY: INTERNAL TECHNOLOGY ACCEPTABLE USE

SECTION: INFORMATION AND TECHNOLOGY

POLICY NO.: 302

EFFECTIVE DATE:

11/08/11

OFFICE OF RESPONSIBILITY: OFFICE OF TECHNOLOGY

THE LANGUAGE USED IN THIS POLICY IS NOT INTENDED TO CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE STATE DEPARTMENT OF EDUCATION. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENTS OF THIS POLICY, IN WHOLE OR IN PART, WITH OR WITHOUT NOTICE.

A. Introduction

This Internal Technology Acceptable Use Policy (AUP) has been developed to help protect the system user and the South Carolina Department of Education (hereafter "Agency"). Information is an important Agency asset. Accurate, timely, relevant, and properly protected information is absolutely essential to Agency's business. Properly used, the Agency's information processing systems support the Agency by improving its productivity, and help the Agency to meet its mission. This policy is intended to ensure that the systems and related data are not subverted.

B. Policy Statement

The Agency's network and computers are intended for authorized users only. Users of the network and all computer equipment have no expectation of privacy in their use of this network or equipment. Use of the agency's network and its computers constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network or on the local computer for any purpose including employee disciplinary action and/or criminal prosecution.

No employee should have any expectation of privacy as to his or her system, Internet, or electronic mail usage. Additionally, State law requires the Agency's Internal Technology staff to report to authorities the names of any individuals who have sexually explicit materials involving minors on their computer.

Storage and bandwidth are expensive and are reserved for business purposes. Data, files, and e-mail stored on the agency's network and computers are the property of the Agency and may be confiscated or scanned at any time. An employee's data transmissions and software may be periodically monitored and audited to ensure adherence to agency standards. The network's security systems are capable of recording each Web site visit;

each chat, newsgroup or electronic mail message; and each file transfer into and out of our internal networks, and the agency reserves the right to do so at any time.

Agency desktop computers, laptops, mobile technologies (PDAs), and other peripheral devices, while usually individually assigned, are agency property. They are to be used for Agency business and will not be used for the personal benefit of any employee. However, some incidental personal use of computers, consistent with the Ethics, Government Accountability, and Campaign Reform Act, S.C. Code Ann. § 8-13-700 (Supp. 2002), is permitted.

Sensitive data should be stored on the network in order to be protected against unauthorized access. Sensitive data stored on any local machine's hard drive should be placed in encrypted folders. Sensitive data stored on any mobile equipment (laptop and/or CDs, USB drives, etc.), must be placed in encrypted folders to protect against unauthorized access should the equipment or storage device become lost or stolen.

C. Definitions

System—Any system or network, including associated hardware and software, managed, administered, or controlled by the Agency or its assigned entities.

1. **System User.** Any Agency regular employee, intern, temporary employee, consultant, contractor, or any other person who has been granted access to any Agency information processing system.
2. **Information Asset.** Any data, information, or material generated, gathered, or compiled by Agency system users, regardless of electronic, magnetic media, or hard copy form, including online services. These assets are considered to be Agency property.
3. **Physical Assets.** Any hardware or media, or components thereof, owned, leased, or rented by the Agency and used to support information assets and/or those the Agency serves.
4. **Internet E-mail.** Any electronic messages transmitted through third party e-mail system providers via the Internet rather than the Agency's provided or established internal e-mail system (e.g., Google mail, Yahoo)
5. **Malware.** Malicious software such as viruses, worms, Trojans, etc.
6. **Virus.** A computer virus is an unauthorized program that replicates itself and spreads onto various data storage media (e.g., USB drives, magnetic tapes) and/or across a network.

D. Summary of System User Responsibilities

All system users accessing and using electronic information have the responsibility to

1. comply with all Agency information Computer Systems policies and procedures (electronic or otherwise).
2. report any known, suspected, or potential policy violations to the IT Director, either directly or through their office director or divisional leader.
3. to only use Agency physical and information assets for legitimate Agency purposes (within the scope of their job responsibilities). Under no circumstances shall system users transfer data to or from non-Agency sites or individuals unless the transfer has been authorized by Agency management (in accordance with this policy).

E. Specific Policies for System Users

The previous sections defined the Agency's Acceptable Use Policy. This section provides specific policies and guidelines for all system users.

Wherever possible, the IT office will rely on the systems to enforce these policies, but user cooperation is essential. The systems themselves have various monitoring and auditing features, which will also be used to ensure compliance. Any questions about these policies or their meaning should be referred to management.

1. Password/Account Management

Controlling access to the Agency's systems is essential—both to protect the Agency's information resources and to protect certain data that the Agency manages. This need becomes increasingly vital as the systems are entrusted with more sensitive and valuable information. Thus, the Agency has the need to accurately establish the identity of any user accessing a system. As a result, effective use of login accounts and passwords is perhaps the single most important, but not only, security responsibility of users.

a. Password Composition

- (1) All passwords must have at least eight (8) characters.
- (2) All user-chosen passwords must contain at least one numeric character (0–9).
- (3) All system users must choose passwords that cannot be easily guessed. This means that passwords must not be

related to the user's job or personal life. For example, a car license plate number, a spouse's name, an address, a word found in the dictionary, or terminology common to the Agency should not be used.

- (4) Your password must not be the same as, or include, your sign on username.
- (5) System users should not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. (For example, users should not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.) In addition, system users should not construct passwords that are identical or substantially similar to passwords that they have previously employed.

b. Changing Passwords

- (1) All system users must change their passwords at least once every year.
- (2) All passwords must be promptly changed if they are suspected or known to have been disclosed to unauthorized parties.

c. Storing Passwords

- (1) Passwords must not be written down and left in a place where another person might discover them.
- (2) Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.

d. Password Sharing

- (1) Regardless of the circumstances, passwords should not be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to be responsible for actions that the other party takes with the password. The owner of an assigned user account is responsible for all activity that occurs in association with their user account.

- (2) If system users need to share computer resident data, they should use electronic mail, public/shared directories on local area network servers, secure Web interfaces, and other mechanisms.
- (3) For assistance with legitimate needs to share data, the advice of IT staff should be sought.

e. Log-in Sessions

- (1) Unattended Sessions. System users should not leave their computer (PC) workstation unattended without first logging out or ensuring a password-protected screen saver/electronic lock is turned on.
- (2) Using another system user's electronic mail (E-mail) account. System users must not use an electronic mail account assigned to another individual to either send or receive messages unless specifically authorized by the owner of the account. The owner of the account remains liable for any use or misuse of the owners account if the owner allows access to the account by another party.

2. Use of Systems

a. Personal Use of Systems

Agency computer and communications systems must be used for authorized Agency business purposes only. Software for playing games (or engaging in any similar social activity) may not be stored or used on any Agency computer systems.

b. Electronic Mail (e-mail)

- (1) E-mail systems are intended to be used solely for Agency business purposes. E-mail systems may not be used for unlawful activities, including violation of copyright laws or violation of any license agreements.
- (2) E-mail systems may not be used for any type of solicitation other than those directly related to Agency business activities. This restriction includes any political, non-agency authorized charitable, social, or personal purposes.
- (3) E-mail users will not send or disclose Agency confidential or sensitive information to anyone without the need to

know. Under no circumstances will the use of Internet e-mail be used to send any Agency confidential or sensitive information to any persons unless the e-mail is encrypted.

- (4) In addition, creation or forwarding e-mail of sexually explicit or offensive messages, cartoons, jokes, ethnic slurs, or racial epithets is strictly forbidden.

c. Use of Non- Agency Systems

System users must not use or install non-Agency computers, computer peripherals, or computer software into Agency facilities or equipment without prior authorization from the Agency CIO, IT Director, or their designee.

d. No Unauthorized Multi-user Systems

System users must not establish local area networks, wireless access points, switches, routers, modem connections to existing local area networks, or other multi-user systems for communicating information unless explicitly authorized by the IT Office.

e. Reporting Changes in User Employment

Each office director must notify the IT office immediately upon termination of any employee with a network and/or e-mail account. This includes consultants and temporary employees as well as full-time employees. This may be done by contacting IT Support. The inactive accounts may be retained for a period not to exceed 30 days. At that time, e-mail and network accounts, including all of the employee's files and e-mail, will be deleted.

The office director may request a CD-ROM of the terminated employee's files before the end of the 30-day period. The director may also request access to the employee's e-mail during the 30-day period in order to print or forward needed e-mail.

Employees anticipating leaving the agency are encouraged to clean out unnecessary e-mail and network-stored files and distribute needed items to appropriate personnel.

3. Computer Software

All software purchased by the agency or its offices must be approved by the CIO/IT officer pursuant to Agency procurement policies. Unauthorized use or copying of software licensed to the Agency is strictly prohibited.

Only authorized computer software should ever be used on Agency systems. This is to protect the Agency from potential liability resulting from using unlicensed software and to ensure that systems are not damaged by malicious computer programs such as viruses.

a. Eradicating Computer Viruses

- (1) If users suspect infection by computer malware, they must stop using the involved computer, unplug network cable, and immediately contact IT Support for assistance. Because viruses have become very complex, users must not attempt to eradicate them from their systems.
- (2) IT will provide anti-virus checking software on all Agency computer systems. Under no circumstances will an employee turn off or otherwise disable this software.

b. Installing Software

- (1) System users must not attempt to download and install software from external electronic mail systems, external communication networks (including the Internet), or other systems outside the Agency, except as approved by IT. This prohibition is necessary because such software may contain malware and may damage Agency information and systems.
- (2) System users may not place any computer program developed outside of the Agency on any system unless the program has first been approved by the Agency.

c. Making Copies of Software

Third-party software in the possession of the Agency must not be copied unless such copying is consistent with relevant license agreements and either

- (1) Management has previously approved of such copying, or
- (2) Copies are being made for contingency planning purposes.

d. Agency Computer-Related Software and Documentation

- (1) All software, documentation, and data developed or inputted on or for Agency computer applications is considered Agency-sensitive material and must not be taken elsewhere when an employee, consultant, or contractor leaves the employment of the Agency.
- (2) Without specific written exceptions, all data, programs, or documentation generated by or provided by employees, consultants, or contractors for the benefit of the Agency are the owned property of the Agency.

e. Testing Systems Security

- (1) System users must not test nor attempt to compromise internal system controls.
- (2) Unless specifically authorized by the IT Officer or designee, system users must not possess or use software or hardware tools that can be used to break security mechanisms. Examples of, but not limited to, such tools are those that facilitate illegal copying of copy-protected software, discovery of secret passwords, collection or

examination of network data packets, or unauthorized decipherment of encrypted data.

f. Use of Information for Non-Business Purposes

Agency information assets (including product specifications, databases, mailing lists, internal software, computer documentation, etc.) must only be used for the business purposes specifically allowed by management. Use of these information assets for any other reason will be permitted only after written permission has been granted by the IT Director or their designee.

4. Privacy Rights

a. Right of Management to Examine Data

All data stored in and all messages sent over Agency computer and communications systems are the property of the Agency. To properly maintain and manage this property, the Agency reserves the right to examine all data stored in or transmitted by these systems. Since all of the Agency's computer and communication systems are for business purposes only, system users should have no expectation of privacy associated with the information they store in or send through these systems, including electronic mail.

b. Logs

Where possible, IT will log all actions system users perform on any multi-user system. These logs provide the required audit trail that will meet security regulations. In addition these logs will provide the data used to investigate and resolve unusual system conditions or used in the event of a security investigation.

c. Electronic Mail

Agency management may, at its discretion, access and disclose any electronic mail message.

d. Freedom of Information Act

Information stored on Agency computers and systems, including but not limited to e-mail, are subject to disclosure under the South Carolina Freedom of Information Act, unless the content is specifically exempted from disclosure pursuant to that act.

5. Confidentiality Policies

a. Transportable Computers and Media.

System users in the possession of portable, laptop, notebook, palmtop, or other transportable computers containing sensitive Agency information must not leave these computers unattended at any time unless the information has been encrypted. Such computers must not be checked in airline luggage systems but must remain in the possession of the traveler as hand luggage. In addition, these systems must be protected by any available boot-password facilities.

b. Removal of Sensitive Information

Agency information may not be removed from the Agency's premises except when there is a business requirement to do so. This policy includes portable computers with hard disks, USB drives, hard-copy output, paper memos, and the like. An exception is made for authorized off-site back-ups or authorized tele-commuting.

c. Disclosure of System Controls and Assets

System users must not disclose to any persons, inside or outside of the Agency, the information system controls that are in use or the way in which they are implemented. Exceptions will be made on a need-to-know basis only by IT management.

d. System Browsing Prohibited

System users must not browse through Agency computer systems or networks. For example, curious search for interesting files and/or programs in the directories of other Departments or users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing.

6. Theft/Loss of Equipment

Employees are expected to apply due diligence in securing their assigned computer equipment and peripherals from access by non-authorized persons, from loss, and from possible theft. The employee must immediately report the loss or suspected theft of a computer and/or its peripherals to his or her immediate supervisor and to IT. The report must be made by the next business day following the determination that the equipment is missing. If the loss is a result of the employee's negligence,

the employee may be required to reimburse the agency for the replacement cost of the leased or agency-owned equipment.

F. Internet Services

By its nature, the Internet connection and services supported are a tremendous security threat to the Agency's computer systems (and the data contained within them). The IT office has made great efforts to provide a secure firewall between the Agency's networks and the Internet. This firewall is designed to keep "hackers" from compromising the Agency's networks and disrupting the day-to-day Agency operations.

Unfortunately, no firewall can prevent abuse or bad judgment on the part of any user that is authorized to access these Internet services. This potential for damage to Agency assets is the exact reason why access to the Internet is monitored.

1. Internet and Your Data

- a. The Internet is an unsecured network. All data sent across the Internet is sent in clear text. This means any e-mail messages, files transferred, and so forth are sent in such a manner that anyone can read the information.
- b. The Internet is not to be used to transfer any Agency sensitive or confidential information without approved security practices being performed. When in doubt, do not send the data across the Internet.

2. Passwords and the Internet

If you access any Internet sites requiring a password, do not use any password that you use on an Agency computer system. Always select "No" if prompted by the Internet to save or remember a password.

3. Internet File Transfers

- a. One threat the Agency has to deal with on the Internet is the potential of malware being brought into our internal networks. Malware can be brought in when files are transferred with the File Transfer Protocol (FTP), as attachments to e-mail messages, as un-encoded files attached to a NEWS article, and from "clicking" on files for download from a Web page on a Web site. (Every time you click on anything on a Web page, you download a file to your computer.) No employee is allowed to download any files onto any Agency computer system unless it is work related.

- b. All executable files downloaded from the Internet in any of the above means must be virus checked before being run on any Agency computer system.
- c. No employee is allowed to download upgrades to existing software packages loaded on any Agency computer system unless explicitly authorized by IT.

4. Internet E-mail

- a. Internet e-mail services are intended to be used solely for Agency business purposes. You may not use Internet e-mail for unlawful activities, including violation of copyright laws or violation of any license agreements. Internet e-mail may not be used for any type of solicitation other than those directly related to Agency business activities. This restriction includes any political, charitable, social, or personal purposes.
- b. Under no circumstances will the use of Internet e-mail be used to send any Agency confidential or sensitive information to any persons, unless authorized encryption or security-control software has been properly used.
- c. In addition, creation or forwarding Internet e-mail of sexually explicit or offensive messages, cartoons, jokes, ethnic slurs, or racial epithets is strictly forbidden.

5. Internet Logs

Security requirements mandate that IT maintain detailed logs of all Internet activities. Each and every transaction the user performs on the Internet is logged with the user's name, time of day, and what action has taken place. These logs are reviewed to ensure the security of our Internet connection has not been compromised or to see if there has been improper use of the Agency's Internet services.

6. Inappropriate Use

Inappropriate Use defined. The Agency provides access to the Internet for the purpose of advancing its interests. Use for non-business purposes is prohibited. Unauthorized use includes, but is not limited to, nonbusiness-related streaming of video and/or audio, nonbusiness-related instant messaging and chatting, financial Web sites, online auctions and shopping, pornography, gambling, online dating, personal social networking, and using the Internet services to download, create, store, or disseminate offensive or obscene material.

Employees will not make or use illegal copies of copyrighted software or other mediums, store such copies on state systems, or transmit them over state networks. In addition, employees must be aware of and must respect copyrighted works found on the Internet and will download only items that are public or whose author or owner has given permission to copy. Employees who knowingly violate the copyright law are doing so outside the scope of their employment and will be personally liable for any damages that may result from the unlawful copying.

7. Approved Usage

Incidental personal use of the Internet and e-mail, consistent with the Ethics, Government Accountability, and Campaign Reform Act, is permitted.

8. Reporting of Security Problems

a. Internal Reporting.

All system users have a duty to report all information-security violations and problems to the IT management on a timely basis so that prompt remedial action maybe taken.

b. Immediate Reporting of Computer Viruses.

- (1) Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. Accordingly, if system users report a computer virus infection to the IT office immediately after it is noticed, even if their negligence was a contributing factor, no disciplinary action will be taken.
- (2) The only exception to this early reporting amnesty will be those circumstances where a system user knowingly caused a computer virus to be introduced into Agency systems. However, if a report of a known infection is not promptly made, and if an investigation reveals that certain system users were aware of the infection, these system users will be subject to disciplinary action including termination.

9. Data Backup and Archiving

a. Back-up of Data

Responsibility for Back-ups. All information residing on Agency systems must be periodically backed up. At a minimum, every user is responsible to ensure that all newly created or updated data must be checked into the Agency's document system, copied onto network drives (drive F:\ normally), magnetic tape, or USB drives. The frequency of this backup is dependent on the volatility and the critical nature of the data.

Note: Data located on a local computer's hard drive, normally C:, is not backed up by IT's automated backup systems.

b. Archiving

(1) General Policy

Information sent and received by e-mail is subject to the same retention schedules as other agency records. Employees are responsible for proper maintenance and archiving, where necessary, of electronic documents just as they would be responsible for maintenance and archiving of other documents. The requirements for archiving can be found at www.scstatehouse.gov/coderegs/c012.htm beginning with section 12-300.

(2) Administrative Correspondence Files (Executive Levels)

Description. Correspondence is related to the administration of an agency or division. Communications concern coordination of programs, agency policy, and responsibilities of a non-routine nature that impact on the agency or its divisions. These letters are usually found at the agency director, deputy director and division director levels. These files must be maintained for 3 years after fiscal year. In addition, a selection of needed documentation must be archived at the State Archives permanently.

(3) Administrative Correspondence Files (Non-Executive Levels)

Description. Routine correspondence created or retained below the levels of agency director, deputy director, and division director. Letters and memoranda reflect communications regarding program procedures, general work activities, and responses to information requests. These records must be maintained until no longer needed for reference, then destroyed.

c. E-mail Auto-Deletion

Due to the amount of server space needed to store e-mail, the SCDE e-mail system will be set with an auto-deletion schedule. All email will be deleted from a user's inbox, sent box, or trash after thirty (30) days, if not deleted sooner by the user. E-mail moved by the user into a folder will be retained for ninety days (90) at which time will be automatically deleted. Employees may archive e-mail to retain longer than the above time periods. Employees are individually responsible for archiving any e-mail that is subject to the state required retention schedules as referenced above in Section F(9)(b).

10. Personal responsibility

It is recognized that employees may occasionally use these systems and networks for limited incidental personal use during non-working time.

Such limited personal use may be acceptable as long as other usage policies are followed and the use does not interfere with an employee's work or negatively impact the computer system or network and does not result in additional public expense.

These systems are not available or accessible for public speech or any First Amendment expressive activity or for use by the public; further, the systems are expressly declared not to be a public forum.

By accepting your user identification and password and related information, and accessing the Agency's network or Internet, you agree to adhere to this Policy.

You also agree to report any network or Internet misuse or abuse to your Office or Division leader, or to the Agency's CIO or Internal Technology Director.

Misuse also includes policy violations that harm another employee or another individual's property.

11. Violation of Policy

Employees not in compliance with any of the above Agency Computer System Policies, standards, or procedures will be subject to disciplinary action including suspension and/or termination.